Versterken, verbinden, vooruitkijken

Jaarmonitor NBIP 2024

Colofon

Aan deze uitgave hebben meegewerkt

Octavia de Weerdt
algemeen directeur, Stichting NBIP

Wouter Pegtel
communicatie & public affairs manager, Stichting NBIP

Pim Kokke
communicatiespecialist, Stichting NBIP

Met dank aan

Valerie Frissen
Rick Sulman

Opmaak

Bijdevleet, Rotterdam

Voor meer informatie, zie **www.nbip.nl**

Inhoud

Voorwoord 4

Samenvatting 6

Over NBIP 8

Valerie Frissen: "Het momentum is er nu om vanuit collectieve verantwoordelijkheid de Europese en nationale digitale autonomie te versterken" 9

Missie & Visie 11

Organisatiestructuur 12

Governance 13

Bestuur 14

Rick Sulman: "Het internet houdt niet op bij de grens" 15

Diensten
- Tapdienst 17
- NaWas 19
- Clean Networks 20

Ontwikkeling Deelnemers 22

Cijfers 2024
- Tapdienst 23
- NaWas 25
- Clean Networks 26

Public affairs 27

Octavia de Weerdt: Cyberweerbaarheid is een collectieve zaak 28

NBIP in Europa 30

NBIP & Europa: IPCEI-CIS / MISD 31

Op de zeepkist 32

Terugblik derde editie NBIP NEXT 33

Voorwoord

Octavia de Weerdt
Algemeen Directeur NBIP

2024 was een belangrijk jaar voor NBIP waarin een stevige basis is gelegd voor de toekomst. Die toekomst is in sommige opzichten onzeker: de schuivende panelen op het wereldtoneel vragen meer van de (cyber)weerbaarheid van onze samenleving en dus ook van NBIP. Die weerbaarheid bestaat niet alleen uit een paraatheid ten aanzien van dreigingen, maar ook het vermogen van Europa om haar digitale autonomie vorm te geven.

Net als veel andere organisaties in onze sector, heeft NBIP zich tot deze nieuwe realiteit te verhouden. Gelukkig hebben we in 2024 hard gewerkt aan het verder optuigen van een robuuste en koersvaste organisatie die relatief autonoom haar dienstverlening en expertise levert aan deelnemers, partners en stakeholders. Daarmee staat een solide basis waarop ook in een steeds turbulenter wereld vertrouwd kan worden.

Dat is nodig, want Europa is verwikkeld in hybride conflicten. Zoals we begin 2025 schreven in ons DDoS jaaroverzicht van 2024, die ook is opgenomen in dit rapport, worden daarbij DDoS-aanvallen steeds vaker ingezet om westerse, democratische samenlevingen te ontregelen en angst te zaaien. Ook in het bredere cyberdomein zijn aanvallen, hacks en diefstal van gevoelige data helaas aan de orde van de dag.

We moeten dus weerbaar zijn tegen systematische pogingen tot disruptie, sabotage en ontregeling. NBIP heeft daarom in 2024 haar infrastructuur van forse verbeteringen voorzien en op meerdere plekken extra robuustheid gecreëerd. Dit is inmiddels een doorlopende inspanning binnen de organisatie die steeds wordt afgestemd op de behoeften van onze deelnemers en het (DDoS-)dreigingslandschap.

Nu vrijwel alle grote operationele en strategische veranderingen zijn doorgevoerd (zie ook de vorige NBIP Monitor), bouwen we verder aan onze missie: het bieden van gezamenlijke faciliteiten voor digitale infrastructuuraanbieders, zodat zij hun digitale weerbaarheid en naleving van wet- en regelgeving op orde hebben.

We hebben in 2024 daarnaast ingezet op meer verbinding met onze deelnemers en partners. We hebben onze huisstijl onder handen genomen en een meer toegankelijke 'branding' geïmplementeerd, inclusief een herziening van ons logo en een nieuwe website. We zijn in 2024 gestart met een nieuwe vorm van deelnemersbijeenkomsten (Lunch & Learn) om vaker fysiek met elkaar in gesprek te kunnen gaan. We hebben gesproken op events, in podcasts en deelden onze kennis in media in binnen- en buitenland. Daarnaast hebben we ons eigen event NBIP NEXT in een nieuw jasje gestoken en is de ambitie om dit kennisevent verder uit te bouwen rond de kernthema's van NBIP.

De afgelopen tijd is ook nagedacht over hoe NBIP kan bijdragen aan de uitdagingen waar we met elkaar voor staan. Het creëren en versterken van de digitale autonomie van Nederland en Europa is snel een zeer belangrijk thema geworden. Deze ambitie wordt breed onderschreven en uitgesproken, maar moet liever vandaag dan morgen ook resulteren in concrete oplossingen. NBIP draagt daar via verschillende Europese projecten aan bij, waaronder IPCEI-CIS. Die bijdrage bouwen we de komende jaren verder uit, met als doel collectieve cyberweerbaarheidsvoorzieningen voor de digitale infrastructuur in Nederland en Europa.

Tot slot: in 2026 bestaat NBIP 25 jaar. Dat is een bijzondere mijlpaal voor de stichting, waarbij we trots mogen zijn op wat we als organisatie hebben bereikt voor onze deelnemers en de sector. We hebben ons ontwikkeld tot het expertisecentrum voor DDoS en de mitigatie daarvan, lawful interception en -disclosure, threat intelligence en de bestrijding van online abuse. Dat was niet mogelijk geweest zonder de toewijding en inzet van onze deelnemers, het bestuur en natuurlijk het vernieuwde NBIP-team. Het is heel bijzonder om voorvrouw te mogen zijn van deze toegewijde groep mensen die zich iedere dag inzetten voor een veilig, betrouwbaar en open internet.

Samenvatting

Jaarmonitor 2024

Het afgelopen jaar is er door NBIP gewerkt aan het verder optuigen van een robuuste en koersvaste organisatie die relatief autonoom haar dienstverlening en expertise levert aan deelnemers, partners en stakeholders. Daarmee staat een sterk fundament waarop in een steeds turbulenter wereld vertrouwd kan worden.

Verbinding

Er is een stevig momentum om de strategische digitale autonomie van Europa te versterken. NBIP speelt hier een rol in als ontwikkelaar en verbinder. Concreet betekent dit dat NBIP oplossingen ontwikkelt om de digitale weerbaarheid van de digitale infrastructuursector te vergroten. Daarnaast participeert NBIP in verschillende Europese projecten en samenwerkingsverbanden en levert actief kennis en expertise.

In 2024 heeft NBIP ook veel aandacht besteed aan het versterken van onze verbinding met onze deelnemers en partners. De nieuwe Lunch & Learn bijeenkomsten, waarbij we met deelnemers in gesprek gaan over de laatste ontwikkelingen rondom onze diensten en nieuwe wet- en regelgeving, dragen bij aan het versterken van deze verbinding. Daarnaast hebben we ook meerdere keren in de media onze expertise rondom DDoS-aanvallen en het disruptieve karakter hiervan voor de samenleving benadrukt. Ook het kennisevent NBIP NEXT was afgelopen jaar weer drukbezocht, waarbij we stilstonden bij het tienjarig jubileum van de NaWas.

Versterken

Verbinding gaat samen met het versterken van onze dienstenverlening. Bij de Tapdienst hebben we in 2024 twee nieuwe deelnemers verwelkomt, terwijl het aantal NaWas-deelnemers met acht is toegenomen. Er is afgelopen jaar wel sprake geweest van consolidatie van het totaal aantal deelnemers van NBIP. In een aantal gevallen zijn afzonderlijke deelnemers verdergegaan als één deelnemer. Hierdoor is het absolute aantal deelnemers beperkt gegroeid. Het aantal onderliggende netwerken dat NBIP bedient is echter wel gegroeid, maar dit is dus niet direct terug te zien in het deelnemersaantal.

Ontwikkeling diensten

De belangrijkste ontwikkeling in 2025 en 2026 wordt de technische implementatie van eEvidence binnen de Tapdienst. Deze nieuwe Europese richtlijn en verordening zorgt ervoor dat lidstaten rechtstreeks elektronisch bewijsmateriaal kunnen opvragen bij aanbieders die in een andere lidstaat actief zijn. NBIP heeft met de Tapdienst een uitstekende staat van dienst, waardoor het optimaal is voorbereid op de procesveranderingen. Hierdoor kan NBIP ook deelnemers ondersteunen op het moment dat zij een eEvidence vordering binnenkrijgen.

NBIP zet in op gemeenschappelijke, non profit cyberweerbaarheidsdiensten voor de digitale infrastructuur

Ook de NaWas blijft continu in ontwikkeling. Zo is verouderde apparatuur op het gebied van routing, switching en mitigatielagen vervangen, waardoor de stabiliteit en de capaciteit van de NaWas zijn vergroot. Daarnaast is ook de capaciteit bij diverse internet exchanges vergroot.

De Gedragscode Abusebestrijding, een van de pilaren van Clean Networks, heeft in oktober 2024 een flinke update gekregen. Zo zijn aanpassingen gedaan op het gebied van definities en beleid om deze zo goed mogelijk aan te sluiten op de meest recente (markt) ontwikkelingen en regelgeving. Verder is besloten dat de Gedragscode Abusebestrijding nu jaarlijks, op basis van regelgeving, feedback en ervaringen van de deelnemers aan de Gedragscode, wordt herzien.

Vooruitkijken

De uitdaging voor Europa om haar strategische digitale autonomie te versterken is breed en veelzijdig. Er is sprake van een ongewenste afhankelijkheid van niet-Europese aanbieders bij gebrek aan toereikende Europese alternatieven. Daarom beogen we enerzijds concrete producten en diensten op het gebied van digitale weerbaarheid te ontwikkelen waarmee deelnemers betrouwbare, gemeenschappelijke alternatieven in handen hebben voor niet-Europese diensten. Anderzijds wil NBIP een rol spelen in het aanjagen van onderzoek, innovatie en samenwerkingen in de sector. Een voorbeeld hiervan is onze deelname aan IPCEI-CIS (Important Project of Common European Interest on Cloud Infrastructure and Services) via het MISD-consortium.

Dit alles wordt gedaan vanuit de overtuiging dat een veilig en betrouwbaar internet een gezamenlijke verantwoordelijkheid is. Want door krachten, kennis en middelen te bundelen, organiseren deelnemers via NBIP gemeenschappelijk hun digitale weerbaarheid en operationele naleving van wet- en regelgeving.

Over NBIP

Stichting Nationale Beheersorganisatie Internet Providers (NBIP) zet zich in voor een betrouwbaar internet door aanbieders van digitale infrastructuur te voorzien van gemeenschappelijke diensten. Op deze manier voldoen zij aan de (wettelijke) vereisten en versterken zij hun digitale weerbaarheid. Alles wat NBIP doet, is vanuit de overtuiging dat de internetsector samen sterker staat voor een schoner, veiliger en betrouwbaar internet en dat iedereen daar baat bij heeft.

In 2001 is NBIP opgericht door zes internetproviders (ISP's). De stichting werd in het leven geroepen om uitvoering te geven aan de wettelijke aftapverplichtingen die deze ISP's hadden onder de Telecommunicatiewet. Ruim 20 jaar later bestaat de Tapdienst nog steeds. Deze dienst voorziet in de behoefte van aanbieders om de naleving van de aftapverplichting uit te besteden aan een professionele organisatie waarbij onafhankelijkheid geborgd is. De stichting bouwt, onderhoudt en beheert de infrastructuur en kennis die nodig is om namens deelnemers uitvoering te geven aan tapvorderingen.

Het coöperatieve model van de Tapdienst heeft in 2014 navolging gekregen met de Nationale Wasstraat (NaWas). Deze collectieve oplossing voor de mitigatie van DDoS-aanvallen is naar hetzelfde model als de Tapdienst opgezet. Het collectieve probleem van DDoS wordt door deelnemers aan de NaWas gezamenlijk aangepakt, waarbij deelnemers naar rato bijdragen aan de instandhouding, onderhoud, vernieuwing en uitbreiding van de dienst. De dagelijkse operatie is in handen van in networking en DDoS gespecialiseerde engineers in dienst van de stichting.

In 2022 is een volgende dienst gelanceerd: Clean Networks. Dit platform informeert deelnemers over beveiligingskwetsbaarheden en abuse zoals botnets of spamservers in hun netwerk. Deelnemers ondertekenen de sectorale gedragscode internet abuse, sectorbrede afspraken waarmee providers zich committeren aan het voorkomen, opsporen, mitigeren en verwijderen van abuse en kwetsbaarheden in hun netwerk. Clean Networks fungeert tevens als sectoraal Cyber Security Incident Response Team (CSIRT).

In het verlengde van deze activiteiten heeft NBIP zich ontwikkeld tot expertisecentrum voor lawful interception en lawful disclosure, DDoS en mitigatie daarvan en internet abuse en detectie en mitigatie van beveiligingskwetsbaarheden in de dagelijkse operatie van providers. Er wordt nauw samengewerkt met verschillende partners, waaronder brancheorganisaties, de overheid, coalities en publiek-private samenwerkingen op zowel nationaal als Europees niveau.

“Het momentum is er nu om vanuit collectieve verantwoordelijkheid de Europese en nationale digitale autonomie te versterken.”

In gesprek met

Valerie Frissen
Directeur SIDN Fonds

Valerie Frissen is directeur van het SIDN fonds, dat projecten ondersteunt die bijdragen aan een sterk, open en vrij internet. Daarnaast is ze bijzonder hoogleraar Digitale Technologie en Sociale Verandering bij Universiteit Leiden. In 2024 kreeg ze de Lifetime Achievement Award van de Internet Society Foundation uitgereikt voor haar verdiensten in de sector.

Kan je vanuit jouw verschillende expertises een perspectief geven op hoe de internetsector sinds begin deze eeuw is veranderd?
“Dat is altijd een beetje moeilijk, omdat je met name kijkt door de bril die je nu op hebt. Vanuit het perspectief van het SIDN fonds denk ik dat we nu vooral goed moeten nadenken over hoe het internet structureel in elkaar zit en of dat nog steeds goed werkt. Dat hebben we namelijk ooit ontworpen met het idee van een aantal kernprincipes (open en een vrijplaats voor innovatie) waar we nog steeds allemaal achter staan, omdat die principes ons in het verleden heel veel hebben gebracht. Maar waar we nu tegenaan lopen is dat de principes van het internet ook ruimte hebben gegeven aan partijen die misbruik maken van die principes en monopolistische trekken zijn gaan vertonen.

Maatschappelijk en economisch gezien heeft dat veel negatieve effecten opgeleverd. Je ziet nu ook dat de discussie rondom soevereine cloud ervoor heeft gezorgd dat de afhankelijkheid van de diensten van een beperkt aantal partijen nadrukkelijker wordt benoemd. Dat is economisch ongezond, maar maatschappelijk gezien ook omdat het internet volledig in ons dagelijks leven is doorgedrongen. Daardoor zijn wij als gebruikers de grondstof voor het verdienmodel geworden. Denk aan alle data over ons gedrag worden gebruikt en hoe algoritmes ons daardoor allerlei kanten opstuurt.

Aan de beleidskant en vanuit de tech community is te lang gedacht dat dit soort ontwikkelingen zichzelf wel reguleren. Daardoor is er te weinig op gestuurd, waardoor we nu in Europa bijvoorbeeld sterk achteruit aan het reguleren zijn. Dat is voor een groot deel noodzakelijk, maar wel erg reactief. Vanuit de sector voelt dat misschien als ‘stijf gereguleerd’ worden en vaak horen we ook dat dit innovatie afremt. Maar je kan ook andersom redeneren dat dit onze kans is om voor de volgende fase, denk bijvoorbeeld aan alle AI-ontwikkelingen, het nu beter te doen en verantwoorde technologieontwikkeling juist als een bron van innovatie zien. Daar proberen we met het fonds ook een steentje aan bij te dragen.”

Sinds 2015 zijn meer dan 400 projecten met steun van het SIDN Fonds van start gegaan. Welke projecten binnen het domein van een open, vrij en betrouwbaar internet staan je het meeste bij?
“We hebben heel veel mooie projecten ondersteund, waardoor het lastig is om er maar een paar op te noemen. Het is goed om te weten dat we begonnen zijn met drie doelstellingen, waarvan het versterken van het internet zelf een van is. De projecten die we samen met jullie van NBIP hebben gedaan zijn mooie voorbeelden daarvan, omdat het vanuit de collectiviteitsgedachte van de sector is geregeld. Zo worden de sector, het internet en de gebruikers er sterker van.

De tweede doelstelling is het versterken van de positie van de eindgebruiker van het internet, waarbij met name wordt gekeken naar de toegankelijkheid voor gebruikers die dreigen buiten de boot te vallen. Een mooi project wat tussen deze twee doelstellingen inzit, is publicroam. Publicroam is een van origine Nederlands initiatief dat z'n oorsprong kent uit de bestaande wifi-roamingdiensten in het onderwijs (eduroam). Publicroam gebruikt dezelfde om burgers overal veilig en privacy by design wifi te bieden, zonder dat ze gebruik hoeven te maken van onveilige open wifi-netwerken. Bij de tweede doelstelling horen ook onze educatieve programma's, zoals HackShield dat kinderen in een game-omgeving 'opleidt' tot cyber agents, een mooi en succesvol voorbeeld van het vergroten van het digitaal bewustzijn bij kinderen.

De derde doelstelling waar het fonds zich voor inzet, gaat vooral over de gevolgen van het internet. Hierbij willen we de goede uitkomsten van het internet versterken en de slechte tegengaan door middel van tools. Op dat vlak hebben we bijvoorbeeld projecten ondersteund die desinformatie en maatschappelijke polarisatie bestrijden. Een mooi voorbeeld daarvan is DuckDuckGoose, dat zich richt op het opsporen en zichtbaar maken van deepfakes."

Waar ligt de sleutel voor de samenwerking voor het versterken van onze digitale weerbaarheid?
"Ik denk dat het samenspel moet zijn tussen alle partijen, van abstract beleidsniveau tot het individuele gebruikersniveau. Vanuit de positie die je hebt, moet iedereen zijn verantwoordelijkheid nemen. Het is goed dat er nu veel gebeurt aan de kant van regulering, waarbij met name Europa het voortouw neemt. Dat vertaalt zich natuurlijk ook naar de nationale wetgeving. Daarnaast denk ik dat de partijen in de sector nog meer elkaar kunnen samenwerken en elkaar niet alleen als concurrent te zien. Als SIDN Fonds werken we daarnaast ook veel samen met andere fondsen in gezamenlijke calls die vooral aan de maatschappelijke effectenkant zit. En individueel kan je ook je digitale bewustzijn van de diensten die je gebruikt, vergroten en vaker alternatieven gaan gebruiken. Het is daarom nu een goed moment om samen met elkaar te zitten om de verantwoordelijkheid die we hebben, met elkaar vorm te geven."

Wat kan Nederland bewerkstelligen in digitale weerbaarheid?
"Nederland is natuurlijk altijd een land dat geweest dat vooraan liep in de digitale mogelijkheden en toegang. Dat heeft er ook voor gezorgd dat alles tijdens de pandemie (2020-2022) goed is blijven doordraaien. We moeten zeker blijven kijken naar de kansen en waar we als Nederland goed in zijn. Maar wat we veel meer zouden moeten doen, en dat speelt bij de discussie rondom digitale autonomie heel sterk, is de risico's van onze afhankelijkheid binnen de vitale digitale infrastructuur te adresseren. De overheid kan bijvoorbeeld echt een rol pakken als launching customer zijn en in hun inkoopbeleid veel meer sturen op wat je nodig hebt voor de toekomst en hierop eisen gaat stellen voor aanbieders. Dat geldt ook voor publieke sectoren, zoals zorg en onderwijs die massaal op de systemen van een enkele aanbieder zitten. Je moet in deze transitiefase strenger zijn in wat je inkoopvoorwaarden zijn en uiteindelijk bewegen naar de realisatie van alternatieven en investeren in Nederlandse partijen. Dat vergt ook kennis vanuit de overheidskant."

Ligt op het kennisniveau vanuit de overheidskant ook het risico?
"Ik denk dat dit in de laatste jaren wel is verbeterd, maar de overheid stond er niet echt om bekend dat ze deze kennis in huis hadden. Dat werd uitbesteed aan de grote leveranciers, en dat is best risicovol omdat die je in hun systemen proberen te krijgen en behouden. Als je zelf dan niet kan beoordelen of je dat ook daadwerkelijk wil, dan wordt het ook lastiger om eruit te stappen."

Hoe zorgen we als samenleving, sector en overheid ervoor dat we over een aantal jaar als de storm is gaan liggen niet gaan vervallen in oude patronen?
"Het verschil met voorheen is dat de geopolitieke situatie is veranderd. De veiligheidsvraagstukken zijn totaal anders, nu vrede geen vanzelfsprekend perspectief meer is. Daarom zijn we nu de urgentie van een veilige en soevereine digitale infrastructuur veel meer gaan zien. En daarom is het juist nu, omdat het hoog op de agenda bij iedereen staat, belangrijk om stappen met elkaar te zetten. Vanuit de bedrijfskant is het bijvoorbeeld interessant om na te denken over de rol van start- en scaleups. In een open markt worden deze succesvolle pioniers op een gegeven moment gekocht door de grote partijen. Je moet dus ook gaan kijken naar hoe je – als je een zekere mate van digitale autonomie in Europa en Nederland wil – deze partijen en de vitale diensten die zij leveren ook autonoom kan houden."

NBIP en het SIDN Fonds werken op diverse vlakken samen, waarbij Clean Networks een van de projecten is die steun vanuit het fonds heeft ontvangen. Hoe kijk je naar de samenwerking tussen beide organisaties?
"Zeer goed. We kunnen bijvoorbeeld individuele projecten ondersteunen met partijen uit jullie en ook gedeeltelijk onze achterban, maar die komen toch wat moeilijker los. Dan is een organisatie als NBIP voor ons een hele goede partij om mee samen te werken, omdat we vanuit hetzelfde gemeenschappelijke belang – het versterken van de sector en digitale infrastructuur in z'n geheel – samenwerken en innovatie stimuleren."

Missie en Visie

NBIP biedt aanbieders van digitale infrastructuur collectieve compliance- en cybersecuritydiensten die onmisbaar zijn vanwege beschikbaarheid of wettelijke vereisten. Door krachten, kennis en middelen te bundelen, organiseren deelnemers gemeenschappelijk hun digitale weerbaarheid en operationele naleving van wet- en regelgeving.

"Samen sterker voor een betrouwbaar internet."

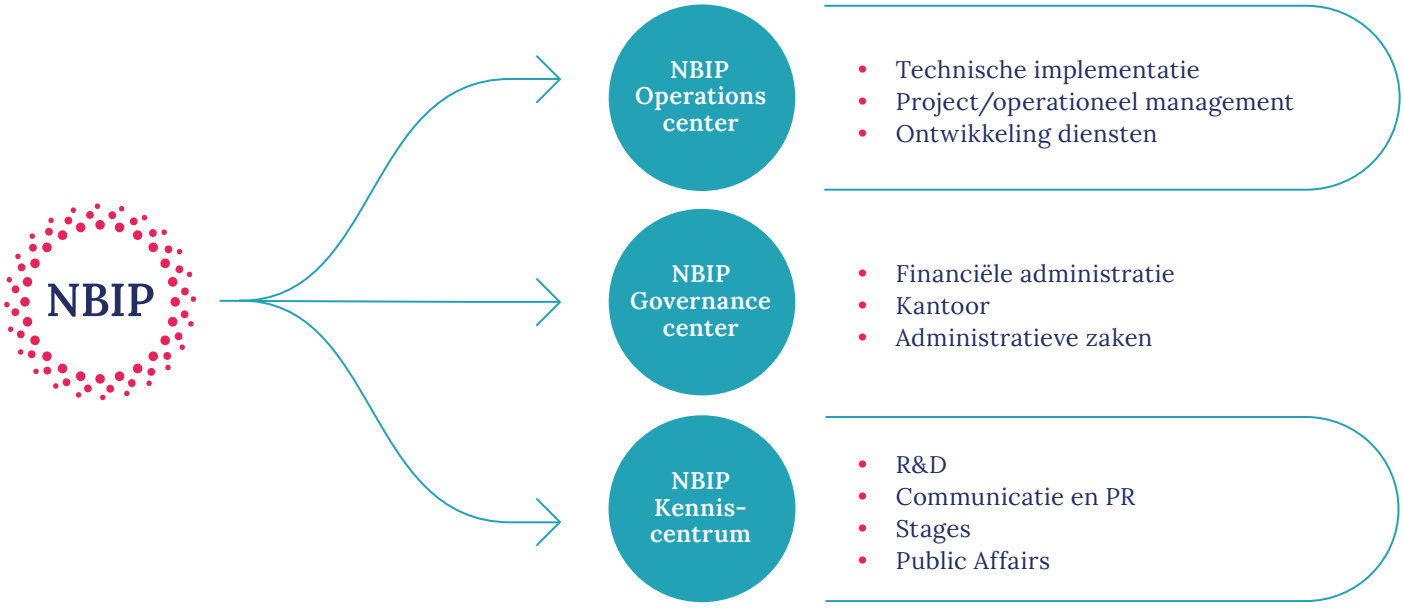
De diensten die NBIP biedt, zijn voor deelnemers dan ook efficiënter collectief te exploiteren dan individueel. Dankzij deze gezamenlijke aanpak hebben zowel grote als kleine aanbieders op een laagdrempelige en kostenefficiënte manier hun zaken op orde.
Aan de basis van de non-profit opzet van NBIP staat het beginsel dat samenwerking de belangrijkste manier is sterker te staan voor een betrouwbaar internet. NBIP levert haar collectieve diensten vanuit de gedachte dat een veilig internet een gezamenlijke verantwoordelijkheid is, en werkt daarom zonder winstoogmerk om dit doel te bereiken.

Organisatiestructuur

De diensten van NBIP worden geleverd vanuit het operations center. Dit is het hart van de organisatie. Daarnaast heeft NBIP een governance center, van waaruit aansturing, finance en administratieve zaken worden georganiseerd, en een kenniscentrum dat zowel op de internetgemeenschap als het bredere publiek is ingericht.

Het NBIP Governance centrum levert ondersteunende diensten voor NaWas, Tapdienst en het Clean Networks Platform waaronder de financiële administratie, bredere administratieve taken en bestuurs-ondersteuning.

Het NBIP Kenniscentrum zet zich in voor de ontwikkeling van kennis, techniek en medewerkers. Het kenniscentrum richt zich op NBIP-deelnemers, de internetgemeenschap en de overheid. Daarnaast fungeert het kenniscentrum in toenemende mate als aanspreekpunt en kennisbank voor media en het bredere publiek op de domeinen waar NBIP actief op is. Denk hierbij aan position papers over digitale autonomie, technische informatie over DDoS mitigatie, achtergrondartikelen over cyber weerbaarheid en NaWas kwartaalupdates.



Governance

Het bestuur van NBIP is samengesteld uit bestuursleden die tenminste voor de helft voortkomen uit het midden van de deelnemers van NBIP. Het bestuur is verantwoordelijk voor de vorming van beleid, financiële controle en verantwoording en een behoedzame omgang met de stichting en de belangen van deelnemers die erin verenigd zijn.

Het bestuur bestond in 2024 uit vier leden:: een voorzitter, een penningmeester en twee algemene bestuursleden waarvan één het vice-voorzitterschap vervult. In 2024 is het voorzitterschap van de Raad van Deelnemers overgegaan van Bernard Edelenbos, die deze rol ad interim vervulde totdat een opvolger gevonden was, naar Frans ter Borg.

Bestuursleden worden voorgedragen door de Raad van Deelnemers, waarin alle deelnemers van NBIP zijn vertegenwoordigd. Zij kunnen onder meer bij monde van de voorzitter van de Raad van Deelnemers het bestuur bevragen en van gevraagd en ongevraagd van advies voorzien. De voorzitter van de Raad van Deelnemers mag bestuursvergaderingen bijwonen, heeft inzage in notulen van die vergaderingen en heeft als een van de belangrijkste taken om namens deelnemers onderwerpen te agenderen bij het bestuur.

De directie van NBIP is verantwoordelijk voor de uitvoering van het beleid zoals vastgesteld door het bestuur en legt verantwoording af over behaalde resultaten. De algemeen directeur is verder autonoom binnen de uitgezette kaders om haar opdracht uit te voeren. De algemeen directeur geeft leiding aan organisatie, daarbij sinds 2025 ondersteund door een management team.

Bestuur

Ludo Baauw
Voorzitter

Ludo Baauw is voorzitter van NBIP. Als voorzitter leidt hij het bestuur en ziet samen met de bestuursleden toe op de koers van de stichting. Hij staat in nauw contact met onder meer de Raad van Deelnemers, andere stakeholders en partners in de sector. In het dagelijks leven is hij CEO van IMG (Intermax Group).

Rick Sulman
Vice-voorzitter & bestuurslid

Rick Sulman is bestuurslid en vice-voorzitter van NBIP. Als bestuurslid speelt hij een rol in de governance van de organisatie en houdt hij zich bezig met toezicht op ethisch, transparant en effectief bestuur. Daarnaast ziet Rick toe op de belangen van VoIP providers binnen de stichting. In zijn dagelijkse werk is hij CEO van telecom operator Speakup B.V.

Tjebbe de Winter
Penningmeester

Tjebbe de Winter is penningmeester van NBIP. Hij ziet als penningmeester toe op de financiële gezondheid en stabiliteit van de stichting. Met meer dan 25 jaar ervaring in ISP-technologie en netwerken kan hij goed de technische afwegingen en consequenties van de financiële plaat doorzien. Daarnaast is Tjebbe is een van de oprichters en directeuren van Cyso Group.

Mike Janssen
Bestuurslid

Mike Janssen is bestuurslid bij NBIP. Hij zet zich in voor een veilige digitale infrastructuur. Mike richt zich op strategische besluitvorming en versterkt samenwerkingen om cybersecurity-uitdagingen, zoals DDoS-aanvallen, gezamenlijk aan te pakken. Daarnaast is Mike actief als CIO bij ITQ en houdt zich daar bezig met de algemene en digitale strategie.

‘Het internet houdt niet op bij de grens’

In gesprek met

Rick Sulman
Bestuurslid NBIP

Rick Sulman is vicevoorzitter van het bestuur van NBIP en CEO van telecom operator Speakup B.V. Binnen NBIP houdt Rick houdt zich met name bezig met het toezicht op ethisch, transparant en effectief bestuur binnen de organisatie. In het interview blikt Rick kort terug op, en deelt hoe NBIP zich als organisatie de komende jaren verder zal ontwikkelen.

In september 2020 ben je toegetreden tot het bestuur van NBIP. Hoe kijk je terug op de afgelopen jaren?
“Allereerst vind ik het persoonlijk belangrijk en leuk om iets bij te dragen aan het internetcollectief in Nederland. De gedachtegang van NBIP om samen als sector collectief diensten te kunnen organiseren voor iedere aanbieder ongeacht grootte, sprak mij heel erg aan. Daarnaast waren de VOIP-partijen, zoals Speakup, destijds nog niet heel erg vertegenwoordigd binnen NBIP. Daarom heb ik mij destijds kandidaat gesteld voor het bestuur. De afgelopen anderhalf jaar zijn we druk bezig geweest om de diensten van NBIP in eigen beheer te nemen. Dat is een ongelooflijk belangrijke stap geweest voor de organisatie. Nu deze transitie is afgerond, blikken we nog meer vooruit op de toekomst.”

Wat zijn de doelstellingen en de koers voor NBIP de komende periode?
“De wereld van cybersecurity is de afgelopen jaren flink veranderd. Vijfentwintig jaar geleden waren er bijvoorbeeld voornamelijk hackers die af en toe vanuit hun zolderkamer voor wat rottigheid zorgden. Nu zie je dat professionele partijen worden ingehuurd door staten om het internet onveilig te maken. De geopolitieke situatie is veranderd en daar moeten we als NBIP op anticiperen. Het collectief georganiseerd aanbieden van operationele diensten met een non-profit karakter is bijvoorbeeld iets wat in Europa heel weinig of niet gebeurt. Daarom kijken we ernaar om de collectieve aanpak van NBIP meer in Europa ingang te laten vinden.”

In het dagelijks leven ben je ook CEO van telecomoperator Speakup. Hoe kijk je vanuit die positie naar onderlinge samenwerkingen binnen de telecomsector in combinatie met de thema’s waar NBIP actief op is?
“De telecomwereld vrij opportunistisch en met name gericht op de korte termijn. Een tijdje terug ben ik samen met Octavia (de Weerdt, algemeen directeur NBIP red.) naar een meeting in Londen van een overkoepelende internationale VOIP-organisatie, waar Speakup ook bij aangesloten is, gegaan. Je merkt dat wanneer er een grote golf DDoS-aanvallen plaatsvindt, dat iedere partij dan gaat nadenken

> “De geopolitieke situatie is veranderd en daar moeten we als NBIP op anticiperen.”

om ook een oplossing tegen deze aanvallen te organiseren. Tijdens die meeting leggen we uit hoe NaWas al meer dan tien jaar een breed omarmde DDoS-mitigatiedienst is binnen de sector. Het is helaas echter de realiteit dat wanneer er minder aandacht is voor DDoS-aanvallen, de telecomsector het onderwerp laten liggen terwijl er wel enthousiast op het verhaal rondom NaWas wordt gereageerd. De bewustwording rondom de gevaren van DDoS op een hoger niveau krijgen, is daarom een aandachtspunt voor de telecomsector. Daarom probeer ik ook wanneer NBIP bijeenkomsten en webinars organiseert zoveel mogelijk bedrijven uit de sector uit te nodigen om te komen luisteren.”

Hoe kan NBIP zich in Europa nog meer profileren?

“Als je kijkt naar bijvoorbeeld NaWas, dan zou het mooi zijn om in nog meer Europese landen verschillende points-of-presence (PoP) punten te hebben, zodat het verkeer nog gemakkelijker kan worden omgeleid. Daarnaast merken we dat er vanuit Europese instanties met veel interesse wordt gekeken naar het model van NBIP als stichting die operationele diensten aanbiedt. Het zou mooi zijn om dit verder uit te rollen en dat NBIP daar – in welke vorm dan ook - een rol in kan spelen. We hebben namelijk veel expertise in huis, waardoor we zeker een verschil kunnen maken want het internet houdt niet op bij de grens.”

Diensten

Tapdienst

NBIP fungeert als een centraal loket voor lastgevers van vorderingen. In de praktijk betekent dit dat bevoegde lastgevers contact zoeken met NBIP als zij een vordering hebben voor een deelnemer aan de Tapdienst. NBIP draagt vervolgens zorg voor de technische, juridische en administratieve aspecten van deze verzoeken.

Aanbieders van openbare elektronische communicatie-diensten of -netwerken moeten gegevens over klanten kunnen verstrekken of een tap kunnen plaatsen als dat wordt gevorderd door instanties die daartoe wettelijk bevoegd zijn. In Nederland is de wettelijke grondslag hiervoor vastgelegd in hoofdstuk 13 van de Telecommunicatiewet en de Wet op de inlichtingen- en veiligheidsdiensten (Wiv).

De bevoegdheden van de opsporingsdiensten zijn beschreven in het Wetboek voor Strafvordering, Boek I, artikelen 126m tot en met 126nb.

In artikel 126m SV is de telefoon- en internettap vastgelegd als een bijzondere opsporingsbevoegdheid. Deze bijzondere opsporingsbevoegdheid kan volgens de Wet Bijzondere Opsporingsbevoegdheden (Wet BOB) alleen worden ingezet op basis van deze drie titels:

1 Er moet een verdenking zijn dat een misdrijf is begaan (titel VI a);
2 Er moet een redelijk vermoeden dat misdrijven, zoals omschreven in artikel 67 lid 1 Sv,
   - In georganiseerd verband worden beraamd
   - of gepleegd die gezien hun aard of de samenhang met andere misdrijven die in dat georganiseerd verband worden beraamd
   - of gepleegd een ernstige inbreuk op de rechtsorde opleveren (titel V)
3 Er moeten aanwijzingen zijn dat er een terroristisch misdrijf wordt gepleegd (titel V b)

NBIP ontvangt namens de aangesloten deelnemer de vorderingen en controleert ook of de inhoud van de vordering volgens de wettelijke eisen is opgesteld. Wanneer dit zo is, zorgt NBIP er namens desbetreffende deelnemers voor dat er aan de vordering wordt voldaan. Mocht een vordering toch niet voldoen aan de gestelde eisen, dan wijst NBIP de verzoeken af en stelt de aanvrager hiervan op de hoogte.

Alle werkzaamheden die NBIP uitvoert bij het aannemen, verwerken en uitvoeren van vorderingen, gebeurt met strikte naleving van de wetgeving en onder strenge veiligheidsmaatregelen om de vertrouwelijkheid en integriteit van de gegevens te waarborgen.

Toekomstige ontwikkelingen

eEvidence

De komende periode wordt de implementatie van eEvidence binnen de Tapdienst ter hand genomen. Deze nieuwe Europese richtlijn en verordening zorgt ervoor dat lidstaten rechtstreeks elektronisch bewijsmateriaal kunnen opvragen bij aanbieders die in een andere lidstaat actief zijn. Aanbieders die een vordering krijgen moeten vanaf 18 augustus 2026 binnen 10 dagen, of in dringende gevallen binnen 8 uur, de gevraagde gegevens verstrekken. Op dit moment geldt voor dit soort vorderingen vanuit een andere lidstaat een tijdsduur van maximaal 120 dagen waarin aanbieders de gegevens verstrekken.

> “Alle werkzaamheden vinden plaats onder strikte naleving van de wetgeving en onder strenge veiligheidsmaatregelen.”

Binnen Nederland is het Ministerie van Justitie en Veiligheid (J&V) verantwoordelijk voor het implementeren van eEvidence in nationale wetgeving. In Europa wordt een gedecentraliseerd IT-systeem ontwikkeld, waarbij er in iedere lidstaat een aansluitpunt is voor toegang, verzenden en het ontvangen van verzoeken. Hierbij is het belangrijk om te melden dat er géén Europese opslag van gegevens komt. Er komen nationale aansluitpunten voor overheid en dienstenaanbieders. Daarnaast kan een eEvidence bevel alléén via het Nederlandse nationale aansluitpunt aan aanbieders worden verstuurd.

NBIP heeft met de Tapdienst een uitstekende staat van dienst, waardoor zij optimaal is voorbereid op de procesveranderingen. Hierdoor kunnen we ook deelnemers ondersteunen op het moment dat zij een eEvidence vordering binnenkrijgen. Daarnaast zijn we gedurende de implementatie van eEvidence betrokken bij de technische commissie, waarbij we binnen Europa meedenken over de praktische invulling van het systeem. Op deze manier zorgen we ervoor dat onze deelnemers straks naadloos kunnen voldoen aan de nieuwe wetgeving.

ATKM

Sinds 2024 detecteert en beoordeelt de Autoriteit online Terroristisch en Kinderpornografisch Materiaal (ATKM) online terroristisch en kinderpornografisch materiaal.

Wanneer de ATKM oordeelt dat online materiaal terroristisch is, kan zij een verwijderingsbevel uitvaardigen. Aanbieders waarbij dit materiaal wordt gevonden, moeten het materiaal binnen één uur verwijderen of ontoegankelijk maken. Wanneer bij dezelfde aanbieder vaker online terroristisch materiaal wordt gevonden, kan de ATKM een blootstellingsbesluit nemen. De aanbieder moet dan maatregelen nemen om te voorkomen dat opnieuw terroristisch materiaal online verschijnt. Daarnaast kan de autoriteit sancties, in de vorm van bijvoorbeeld geldboetes of een last onder dwangsom, opleggen aan aanbieders die niet voldoen aan de verplichtingen die zijn vastgelegd in de uitvoeringswet verordening terroristische online inhoud (TOI) en de Wet bestuursrechtelijke aanpak online kinderpornografisch materiaal.

Voor kleine- en middelgrote aanbieders van digitale infrastructuur brengt dit veel verantwoordelijkheid met zich mee die gepaard gaat met de nodige extra organisatorische belasting. Aanvullend op de Tapdienst onderzoekt NBIP daarom een loket ter aanvulling op de Tapdienst voor haar deelnemers. Dit nieuwe loket met een notice and take down karakter moet ervoor zorgen dat (nieuwe) deelnemers worden ondersteund bij eventuele bevelen vanuit de ATKM. Concreet zal dit betekenen dat NBIP bevelen namens deelnemers kan aannemen en ervoor zorgdraagt dat de deelnemer met spoed actie onderneemt.

Diensten

NaWas

De NaWas is in 2024 op verschillende manieren verbeterd, waarbij veel aandacht besteed is aan de betrouwbaarheid en continuïteit van de dienstverlening.

2024 was een jubileumjaar jaar voor de NaWas, want de dienst bestond 10 jaar. Van een kleinschalige dienst ontwikkeld door enkele NBIP-deelnemers, groeide het snel uit tot een begrip in de Nederlandse internetsector. Het was daarmee een groot succes: het platform groeide in 10 jaar naar 130 deelnemers in verschillende Europese landen.

In de loop der jaren werden verschillende uitbreidingen van de NaWas gerealiseerd, zowel qua capaciteit als beschikbaarheid en aanvullende diensten en functionaliteit. De architectuur van de NaWas is echter niet wezenlijk veranderd in die 10 jaar, simpelweg omdat daar geen noodzaak toe was.

De afgelopen jaren werd echter steeds duidelijker dat het DDoS-landschap sterk veranderde onder druk van onder meer geopolitieke ontwikkelingen. Aanvallen werden complexer, langduriger en hadden in de breedte van het DDoS-landschap meer impact. Deelnemers deden vaker een beroep op de NaWas en hadden in sommige gevallen te maken met langdurige of herhaalde, geavanceerde aanvallen die het hoofd geboden moesten worden.

Achter de schermen werd daarom gewerkt aan een flinke upgrade van de NaWas met als uiteindelijk doel een betere dienstverlening, verbeterde redundantie en meer capaciteit. Ook werd gewerkt aan verbeteringen ten aanzien van het beheer van de infrastructuur en analytics.

Een groot deel van deze plannen is in 2024 gerealiseerd, waaronder een verbeterde redundantie binnen de infrastructuur en bij de internet exchanges waar NaWas gebruik van maakt. Daarnaast is een sFlow service beschikbaar gemaakt aan deelnemers en is de interne monitoring sterk verbeterd, waarbij engineers onmiddellijk op de hoogte worden gesteld van nieuwe prefixes die via de NaWas worden geleid zodat zij real time kunnen monitoren of de mitigatie succesvol verloopt.

Het team van de NaWas is daarnaast uitgebreid waarbij nu alle benodigde expertise in house aanwezig is, van gespecialiseerde kennis van netwerken en BGP tot de details van zeer uiteenlopende typen DDoS-aanvallen en hoe deze gemitigeerd moeten worden. Daarbij is ook de supportinfrastructuur vernieuwd zodat vragen en verzoeken snel en effectief kunnen worden afgehandeld via een dedicated kanaal.

Diensten

Clean Networks

Clean Networks bestaat uit twee pijlers: een threat intelligence platform voor aanbieders van digitale infrastructuur en een gedragscode waarmee die aanbieders zich toeleggen op het voorkomen en actief opsporen & verwijderen van abuse in hun netwerken.

Noodzaak van Clean Networks

Misbruik van systemen en beveiligingskwetsbaarheden in netwerken van aanbieders van digitale infrastructuur is een belangrijke bron van onrechtmatigheid op het internet. We noemen dit soort misbruik abuse. Hiermee wordt gedoeld op alle activiteiten waarmee infrastructuur van aanbieders wordt gebruikt en misbruikt om bijvoorbeeld cyberaanvallen te coördineren en uit te voeren, data te ontvreemden of illegale content aan te bieden.

Eén van de problemen die aanbieders ondervinden bij het voorkomen van abuse is dat beveiligingskwetsbaarheden niet altijd bekend zijn. Het helpt dus als zij proactief worden geïnformeerd over kwetsbaarheden die in hun netwerk aanwezig zijn. Daarbij is het ook belangrijk voor aanbieders om beleid te implementeren waarmee zij abuse kunnen voorkomen van kwaadwillenden die zich voordoen als legitieme klant of afnemer. Clean Networks biedt een totale aanpak van abuse, van detectie en notificatie tot een gedragscode waarmee aanbieders hun beleid en handhaving op orde hebben.

De totaalaanpak van Clean Networks

Clean Networks biedt aanbieders van digitale infrastructuur een effectieve en bewezen oplossing met een breed draagvlak vanuit de digitale infrastructuursector om abuse op te sporen en te bestrijden. De threat intelligence van Clean Networks geeft aanbieders geautomatiseerde meldingen uit uiteenlopende bronnen van kwetsbaarheden, toegesneden op specifieke IP-ranges binnen het netwerk van de aanbieder. Met die informatie kunnen aanbieders gericht actie ondernemen en het risico op abuse in het eigen netwerk preventief reduceren.

Daarbij helpt Clean Networks ook om te voldoen aan wet- en regelgeving zoals de Digital Services Act (DSA) en Network and Information Security Directive 2 (NIS2) door middel van de Gedragscode Abusebestrijding. Onderdeel van deze gedragscode zijn onder meer een notice and takedown (NTD) beleid en een know your customer (KYC) beleid, vormgegeven op basis van internationaal geaccepteerde standaarden.

Gedragscode Abusebestrijding

Met de Gedragscode Abusebestrijding verbinden providers zich onder meer aan het treffen van maatregelen om abuse in hun netwerken op te sporen en beveiligingskwetsbaarheden te verhelpen. Zij verbinden zich ook aan een notice & takedown procedure, ‘Know Your Customer’ (KYC) beleid en een goede bereikbaarheid voor abusemeldingen. Ondertekenaars van de gedragscode verkrijgen het Clean Networks Keurmerk, waardoor zij bijdragen aan een veiliger digitaal Nederland Zij kunnen daarmee aantonen dat zij de nodige maatregelen nemen om abuse te voorkomen en hebben zo een streepje voor in de markt, aangezien steeds meer organisaties in hun inkoopbeleid eisen stellen aan hieraan. De gedragscode helpt daarnaast bij compliance aan de Digital Services Act (DSA) en Cyberbeveiligingswet (Cbw/NIS2).

In oktober 2024 heeft de Gedragscode Abusebestrijding een update gekregen. Zo hebben we aanpassingen verricht op het gebied van definities en beleid om deze zo goed mogelijk aan te sluiten op de meest recente (markt) ontwikkelingen en regelgeving.

> “Aanbieders die de Gedragscode Abusebestrijding ondertekenen, hebben een streepje voor in de markt”

Verder is besloten dat de Gedragscode Abusebestrijding nu jaarlijks, op basis van regelgeving, feedback en ervaringen van de deelnemers aan de Gedragscode, wordt herzien. Bij elke herziening wordt het versienummer bijgewerkt en worden de wijzigingen gedocumenteerd in de revisiegeschiedenis. NBIP is beheerder van de Gedragscode en verantwoordelijk voor het versiebeheer. In de nieuwe versie zijn ook nieuwe secties toegevoegd: Know Your Customer beleid, Niet-nakoming en de onderschrijvers van de Gedragscode.

Vertegenwoordigers Gedragscode

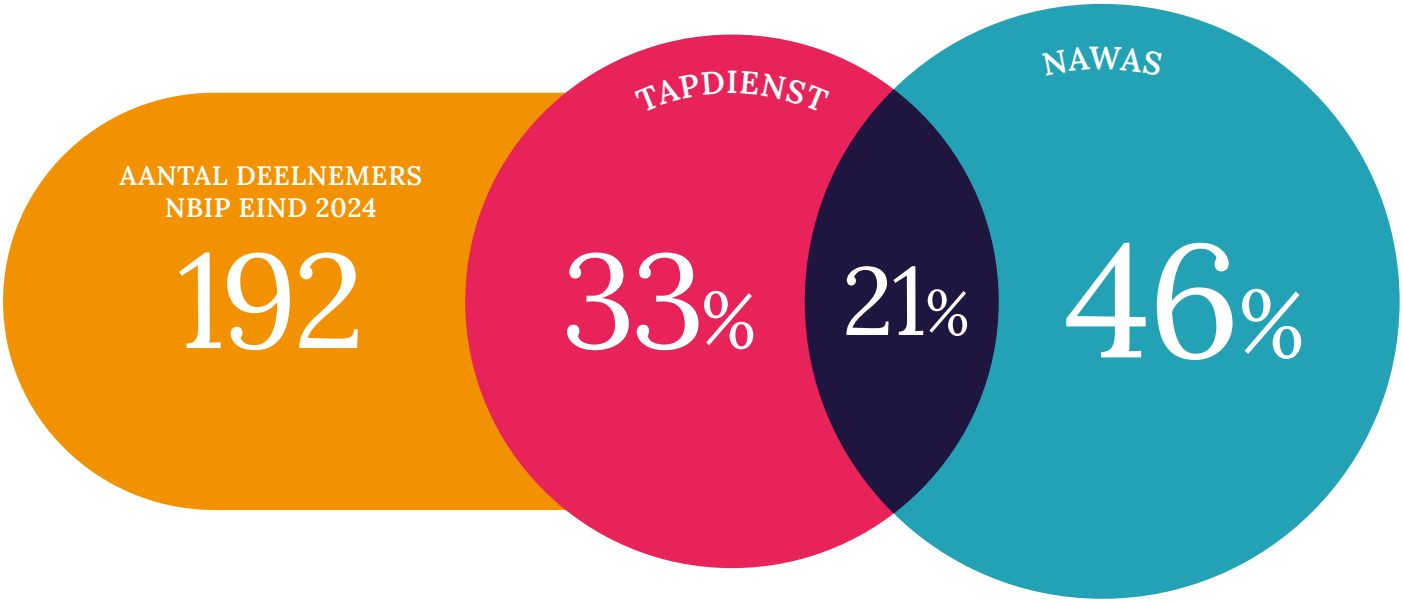
Naast NBIP hebben de volgende organisaties actief bijgedragen aan het opstellen van de Gedragscode: Stichting Digitale Infrastructuur Nederland (DINL), Dutch Cloud Community (DCC), en Vereniging van Registrars (VvR).

Clean Networks is mede mogelijk gemaakt door een subsidie van de Europese Unie en subsidies van het Digital Trust Center en SIDN Fonds.

Ontwikkeling deelnemers

In 2024 is er sprake geweest van consolidatie onder deelnemers van NBIP. De reden hiervoor is dat in een aantal gevallen afzonderlijke deelnemers zijn verdergegaan als één deelnemer. Hierdoor is het absolute aantal deelnemers beperkt gegroeid. Het aantal netwerken dat NBIP bedient is verder uitgebreid.

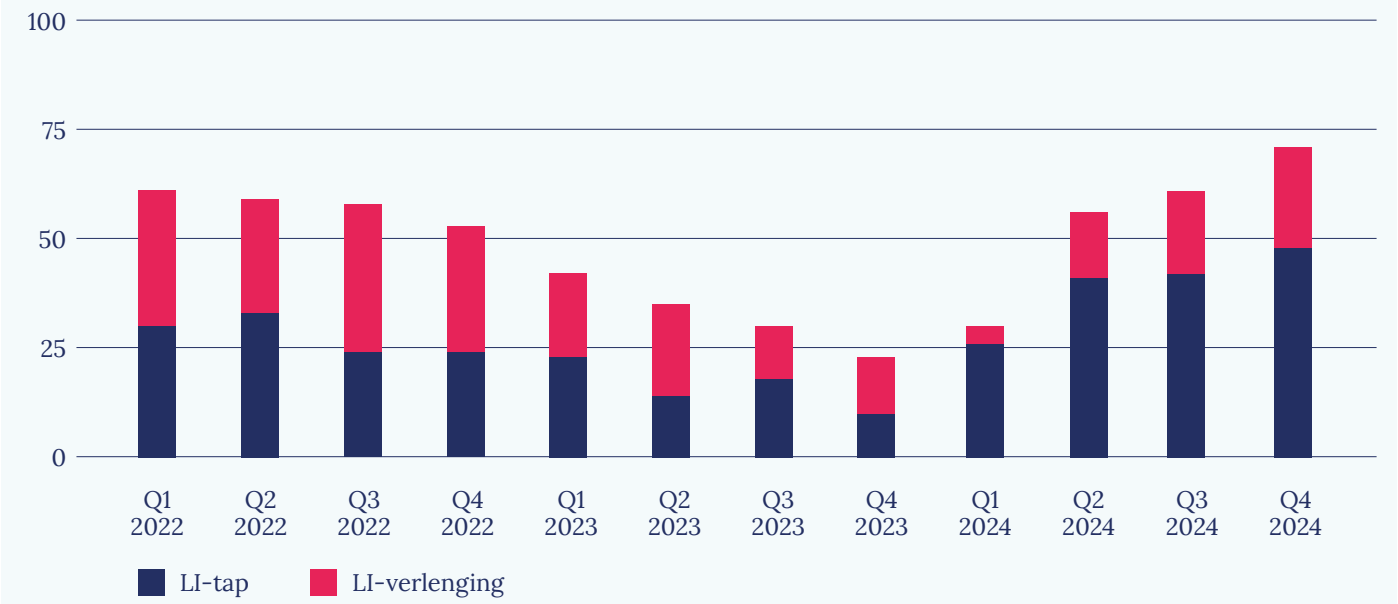
Organisaties die zowel van de Tapdienst als de NaWas gebruikmaken, worden in het totaal aantal deelnemers van NBIP als één enkele deelnemer geteld. Daarom had NBIP eind 2024 ruim 192 deelnemers, waarvan 103 organisaties deelnemen aan de Tapdienst en 129 organisaties deelnemen aan de NaWas. Er zijn 40 organisaties die deelnemen aan beide diensten.



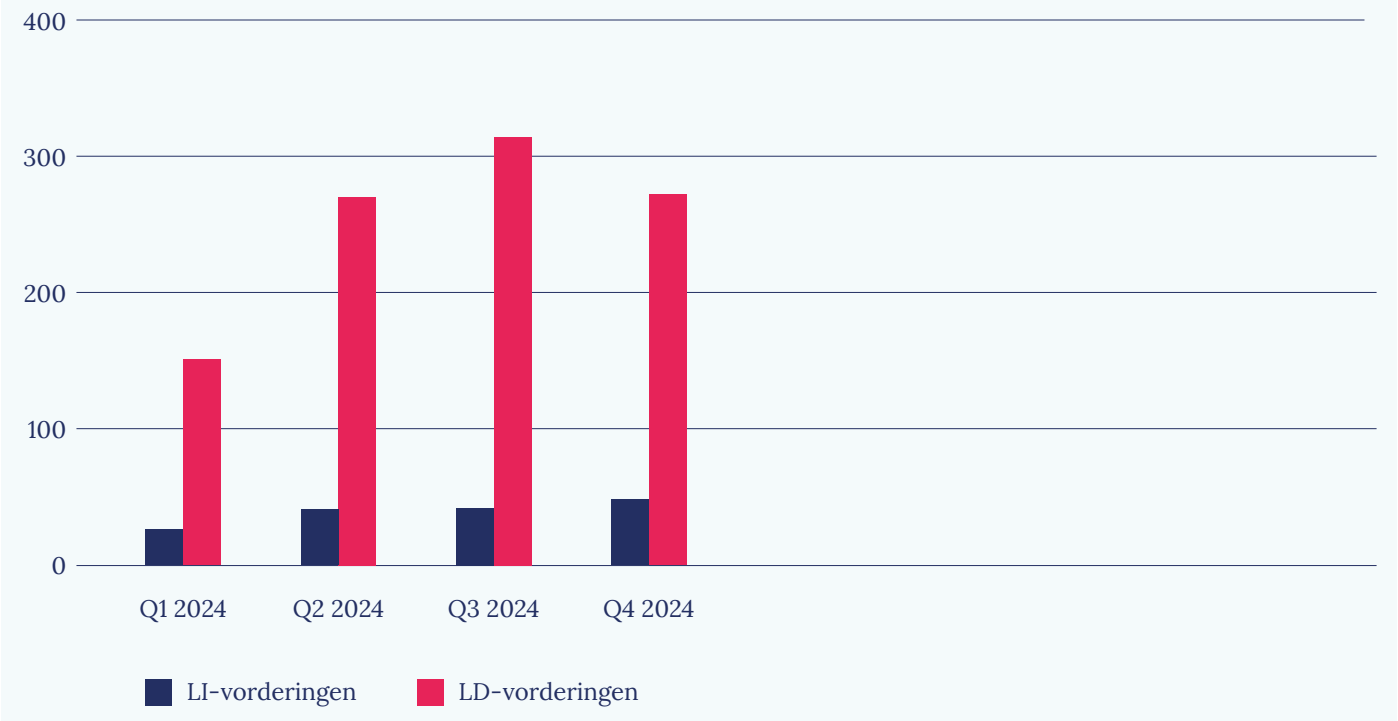
Tapdienst

Cijfers 2024

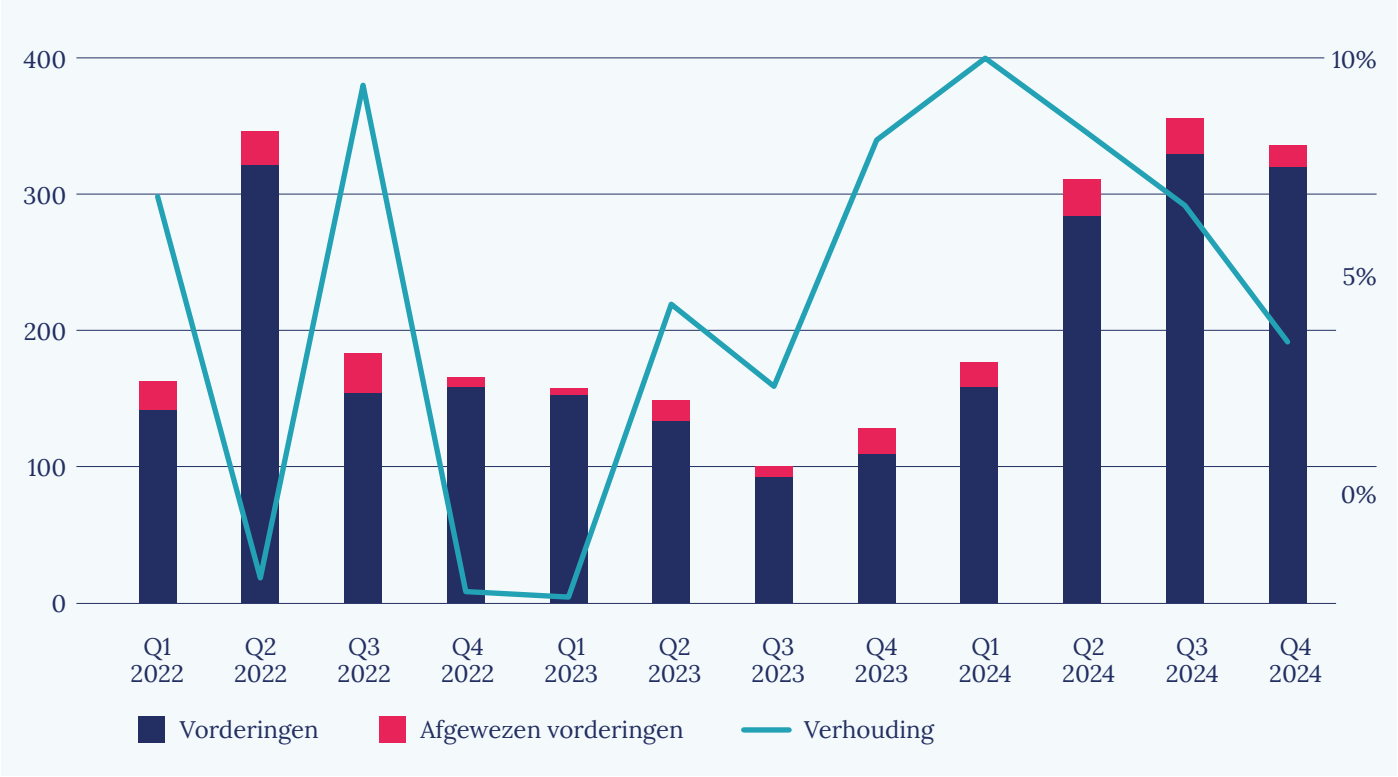
Totaal aantal LI-taps en LI-verlengingen per kwartaal



Aantal LI-vorderingen versus LD-vorderingen per kwartaal



Totaal aantal vorderingen versus afgewezen per kwartaal



NaWas

Cijfers 2024

NaWas statistieken 2024

1933
gemitigeerde aanvallen

5.27
gemiddeld aantal gemitigeerde aanvallen per dag

353 Gbps
maximale omvang

Trends 2024

DNS Amplification aanvallen zijn intensievere geworden. DNS amplification is daarmee in 2024 de meestvoorkomende aanvals vector.

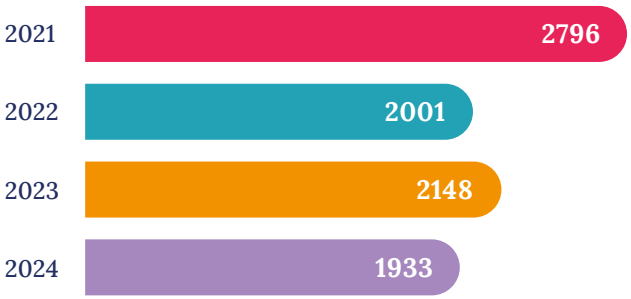
Afname van het aantal aanvallen aan het einde van 2024.

NTP Amplification was consistent een top 3 aanvalsvector.

Top 5 aanvallen in 2024

1. **DNS Amplification**
2. **NTP Amplification**
3. **TCP SYN Flood**
4. **IP low TTL Flood**
5. **UDP HTTP/3 QUIC Flood**

Aantal aanvallen per jaar



Clean Networks

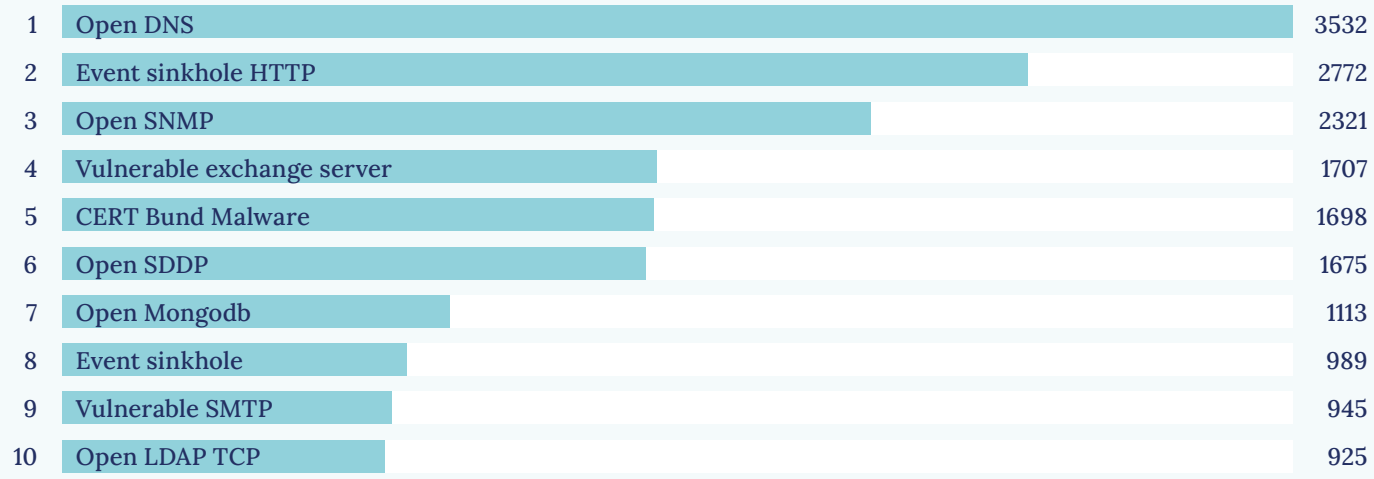
Cijfers 2024

Toelichting

Met Clean Networks verspreidt NBIP informatie over beveiligingskwetsbaarheden en abuse aan aanbieders van digitale infrastructuur. Deze meldingen zijn toegesneden op individuele deelnemers die zich hebben aangemeld voor de threat intelligence feed van Clean Networks, zodat zij gericht kunnen handelen.

In 2023 hebben we **21256** notificaties gedeeld over een totaal aantal van **803764** IP-adressen. In het afgelopen jaar waren dat **8367** notificaties over een totaal aantal van **254132** IP-adressen. Belangrijk om te vermelden is dat in 2023 er werd samengewerkt met een externe organisatie, waardoor óók IP-adressen van niet-deelnemers zijn meegenomen.

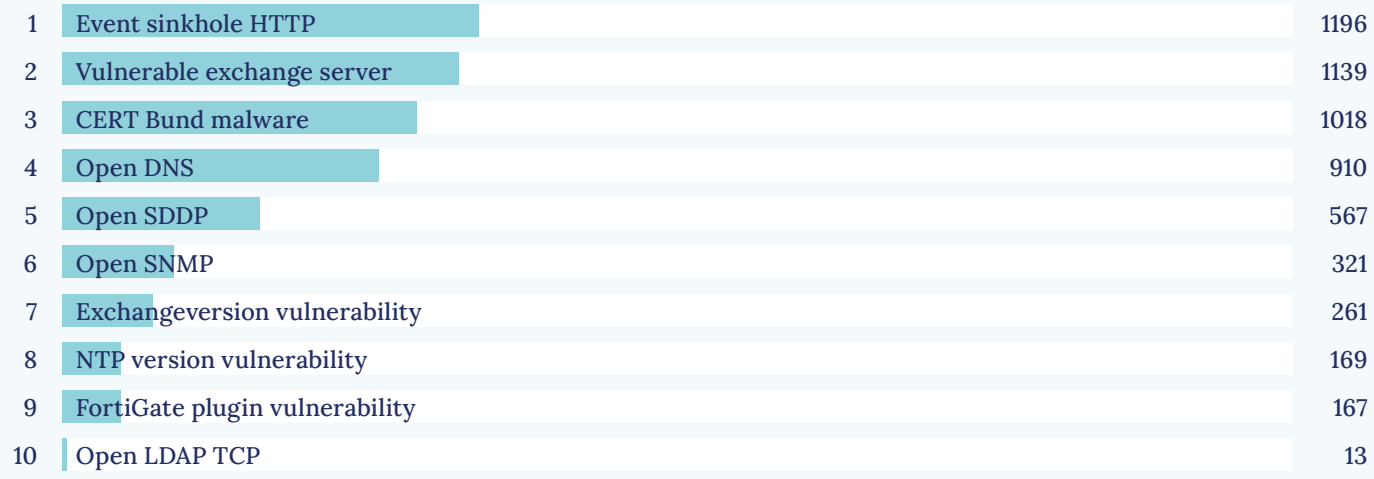
Top 10 Threat Types (gemeten in aantal verstuurde notificaties) 2023



Totaal aantal verstuurde notificaties (2023) — **21256**

Totaal aantal IP-adressen (2023) — **803764**

Top 10 Threat Types (gemeten in aantal verstuurde notificaties) 2024



Totaal aantal verstuurde notificaties (2024) — **8367**

Totaal aantal IP-adressen (2024) — **254132**

Public affairs

NBIP levert waar nodig en relevant graag haar bijdrage aan dossiers die van belang zijn voor haar deelnemers en een veilig en betrouwbaar internet. Dat doet NBIP onder meer door gevraagd en ongevraagd haar zienswijze te leveren op wetsvoorstellen, regelgeving en beleid en deel te nemen in verschillende publiek-private samenwerkingen. NBIP is samen met AMS-IX, SIDN en SURF deelnemer van de koepel Digitale Infrastructuur Nederland (DINL).

De insteek bij de public affairs activiteiten van NBIP is steeds om praktische uitdagingen bij het voldoen aan wet- en regelgeving die spelen bij deelnemers over te brengen aan de juiste overlegtafels. Doordat NBIP ook operationeel actief is met haar diensten, kan het hierdoor een helder beeld schetsen hoe wetgeving en beleid uiteindelijk in de dagelijkse praktijk hun uitwerking hebben.
Dat doen we structureel op vier dossiers.

DDoS-bescherming

Binnen Nederland en Europa positioneert NBIP zich als het (inter)nationale kenniscentrum voor de bescherming tegen DDoS-aanvallen. Door onze jarenlange kennis, uitgebreide ervaring en de NaWas kunnen we van grote waarde zijn voor beleidsmakers. Daarom delen we actief kennis over de aard en omvang van DDoS-aanvallen, effectieve beschermingsmaatregelen en de rol van verschillende partijen in het digitale ecosysteem.

Digitale weerbaarheid in digitale infrastructuur

Door toenemende digitalisering is digitale weerbaarheid een belangrijk domein dat bij veel instanties hoger op de agenda is gekomen. Sectorale samenwerking is daarom cruciaal voor de digitale weerbaarheid in Nederland en Europa. NBIP zet haar expertise op het gebied van DDoS-bescherming, abuse bestrijding en SOC-operaties in om de digitale weerbaarheid te versterken. Gezamenlijke verantwoordelijkheid bij alle partijen in de waardeketen vormt hierbij de sleutel, waarbij NBIP ook pleit voor ruimte in de markt voor het bouwen van innovatieve en praktische oplossingen.

Abuse preventie

NBIP richt zich op het ontwikkelen van best practices en beleidsadvies op de bestrijding van abuse en bad hosting in Nederland en Europa. Onze inzichten op dit domein helpen bij het ontwikkelen van effectieve maatregelen, zonder de open en innovatieve aard van het internet te beperken.

Operationele compliance aan wet- en regelgeving

In de afgelopen 25 jaar heeft NBIP als een van de weinige partijen in Nederland en Europa onafhankelijke expertise opgebouwd in de operationalisering van het uitvoeren van vorderingen en bevelen van daartoe bevoegde autoriteiten voor aanbieders van digitale infrastructuur. We zetten deze kennis in om de operationalisering van deze dossiers voor de digitale infrastructuur op een zo pragmatisch mogelijke manier te borgen.

Column

Cyberweerbaarheid is een collectieve zaak

Door Octavia de Weerdt

DDoS-aanvallen vormen een steeds grotere dreiging. Alleen al in 2025 hebben we aanvallen gezien die Europese Parlementsverkiezingen en publieke diensten en infrastructuur troffen, websites van provincies en gemeenten platlegden en bovendien steeds complexer werden. Om weerbaar te blijven, moeten we dit probleem anders gaan benaderen.

Wapenwedloop in een hybride strijd

DDoS-aanvallen zijn onderdeel van een nieuw normaal dat gekenmerkt wordt door een hybride strijd tussen verschillende geopolitieke machtsblokken. Zij worden nu strategisch ingezet om vrije, democratische samenlevingen in Europa te ontregelen. Niet voor niets trok de MIVD hierover recent aan de bel in hun publieke jaarverslag.

Daarmee is overigens niet gezegd dat recente aanvallen ook allemaal die intentie hadden. Van sommige aanvallen is dit bekend, van andere niet. Maar we weten wel dat de motieven van aanvallers vaak gelegen zijn in vergelding en de disruptieve werking van aanvallen en dat zij die motieven zelf vaak verbinden aan ontwikkelingen op het geopolitieke toneel. Daarmee zijn DDoS-aanvallen al lang geen 'kattenkwaad' of 'digitaal vandalisme' meer, maar onderdeel van een bredere, mondiale strijd.

DDoS en de beschermingsmaatregelen die worden genomen, hebben daarnaast de dynamiek van een klassieke wapenwedloop. Verdediging die vandaag afdoende is, kan morgen worden doorbroken. Door deze dynamiek is het nagenoeg onmogelijk om 100% bescherming te realiseren. En is het een grote opgave om bij te blijven qua kennis en techniek om dit soort aanvallen af te kunnen slaan.

Afhankelijkheid

Het steekt daarbij dat we ons in Europa voor een belangrijk deel afhankelijk hebben gemaakt van DDoS-bescherming van niet-Europese makelij. Want ook op dit gebied is het, net zoals voor veel andere online diensten, slechts een handvol voornamelijk Amerikaanse bedrijven die vrijwel de gehele markt in handen hebben. Als we vinden dat de overheid zich kwetsbaar heeft gemaakt door gevoelige data bij Amerikaanse cloudaanbieders onder te brengen, dan moeten we ook ons afvragen of we onze weerbaarheid tegen cyberaanvallen zoals DDoS niet anders moeten organiseren.

Europese landen hebben er immers alle belang bij om zelf hun digitale weerbaarheid te regelen. Met eigen kennis, technologie en op eigen bodem. Dit is van groot belang voor de digitale soevereiniteit en strategische autonomie van Europa en dus ook Nederland.

> *"Zonder eigen Europese kennis en technologie blijft onze digitale weerbaarheid kwetsbaar."*
>
> ***Octavia de Weerdt***

Het ligt daarom voor de hand om veel meer de samenwerking op te zoeken, binnen Nederland, én binnen Europa. Dat gebeurt in Nederland al in de anti-DDoS-coalitie, waarin overheid en kritieke sectoren samenwerken aan hun weerbaarheid tegen DDoS-aanvallen. Daar is bijvoorbeeld een methodiek ontwikkeld om kenmerken van aanvallen uit te wisselen via een zogenaamd Clearing House, waardoor aanvallen beter herkend en afgeslagen kunnen worden door organisaties die toegang hebben tot dit Clearing House.

In Europa wordt daarnaast in het kader van het miljardenprogramma Important Projects of Common European Interest – Cloud Infrastructure and Services (IPCEI-CIS), gewerkt aan digitale weerbaarheid (security by design) op die plekken waar het er het meest toe doet, namelijk in de digitale infrastructuur van morgen aan de geografische grenzen van Europa. Maar hoewel nuttig en belangrijk, zij beide voorbeelden geen oplossing voor de uitdagingen waar we nu voor staan. Daarvoor is eerst iets anders nodig.

Omslag in denken

We moeten realistisch zijn: zolang veel organisaties hun weerbaarheid tegen DDoS-aanvallen individueel (moeten) organiseren, blijven we als samenleving kwetsbaar. Hier is dan ook een omslag in denken noodzakelijk. We zijn te lang blijven steken in een paradigma waarin individuele verantwoordelijkheid voor digitale weerbaarheid van organisaties de boventoon voert. De nieuwe Cyberbeveiligingswet sorteert voor op een andere manier van denken, maar alleen voor een beperkte groep organisaties. We zullen deze problematiek daarom moeten benaderen vanuit een collectieve verantwoordelijkheid. Commerciële belangen zijn daarbij ondergeschikt aan het bredere, maatschappelijke belang: stabiliteit door de beschikbaarheid van (kritieke) online diensten. En, niet onbelangrijk, het maken van een vuist tegen diegenen die onze samenlevingen en manier van leven proberen te ontregelen. Daar moeten we niet naïef over zijn.

Door krachten te bundelen in initiatieven die onze collectieve weerbaarheid te vergroten, zorgen we dat individuele organisaties overeind blijven. We moeten in Nederlands en Europees verband zelf kennis ontwikkelen, uitwisselen en zelf onze weerbaarheid organiseren, zonder afhankelijkheden buiten onze eigen, Europese sfeer. Dat kan alleen als we anders over DDoS gaan denken en ons verder gezamenlijk organiseren. Het nieuwe normaal hoeft zo geen bedreiging te zijn, maar een belangrijke stap naar een digitaal soeverein en -weerbaar Nederland en Europa.

NBIP & Europa

Er is een stevig momentum om de strategische digitale autonomie van Europa te versterken. NBIP speelt hier een rol in als ontwikkelaar en verbinder. Concreet betekent dit dat NBIP oplossingen ontwikkelt om de digitale weerbaarheid van de digitale infrastructuursector te vergroten. Daarnaast participeert NBIP in verschillende Europese projecten en samenwerkingsverbanden en levert actief kennis en expertise.

De uitdaging voor Europa om haar strategische digitale autonomie te versterken is breed en veelzijdig. Er is sprake van een ongewenste afhankelijkheid van niet-Europese cloudaanbieders bij gebrek aan toereikende Europese alternatieven. Tegelijkertijd bestaan ook op andere vlakken afhankelijkheden die ongewenst zijn en ingezet kunnen worden als geopolitiek drukmiddel, bijvoorbeeld op het gebied van security-oplossingen, dreigingsinformatie en informatie over kwetsbaarheden en abuse.

NBIP onderschrijft de urgente noodzaak van een eigen cloudinfrastructuur voor Europa en neemt daarom deel aan IPCEI-CIS, zoals hierboven beschreven. De noodzaak voor eigen, Made in Europe cybersecurity en cyberweerbaarheidsoplossingen is echter minstens zo groot, aangezien deze oplossingen onze gegevens en systemen veilig dienen te houden. Ook op dit vlak is te veel afhankelijkheid onwenselijk.

Deze problemen kunnen alleen opgelost worden als succesvolle sectorale en cross-sectorale samenwerkingsverbanden gesmeed kunnen worden en de overheid zowel beleidsmatig als financieel in de middelen voorziet om onze digitale afhankelijkheid van niet-Europese partijen af te bouwen.

In de praktijk betekent dit dat de huidige inzet van de EU op meerjarige programma's om Europa's eigen cybercapaciteiten te verbeteren en uit te breiden de belangrijkste manier is om dit soort samenwerkingen te creëren en stimuleren. Maar er is meer nodig. NBIP beoogt enerzijds concrete producten en diensten te ontwikkelen waarmee deelnemers betrouwbare alternatieven in handen hebben voor niet-Europese diensten. Anderzijds wil NBIP een rol spelen in het aanjagen van onderzoek, innovatie en samenwerkingen in de sector.

NBIP & Europa:

IPCEI-CIS / MISD

NBIP neemt deel aan het IPCEI-CIS (Important Project of Common European Interest on Cloud Infrastructure and Services) via het MISD-consortium. In dit consortium nemen zeven organisaties deel, ieder met een eigen specialisatie, waarbij NBIP het cybersecurity aspect voor haar rekening neemt.

In het kort: wat is MISD?

Het doel van het Modular Integrated Sustainable Datacenter (MISD) project is om een nieuw modulair, duurzaam en secure by design ontwerp te ontwikkelen dat ingezet wordt op plekken dichtbij eindgebruikers (edge computing). De innovaties en ontwikkelingen die worden gerealiseerd binnen het project, komen samen in een gevalideerde, gedistribueerde opstelling in een field lab. De looptijd van het project is 5 jaar, van 2024 tot 2029.

De rol van NBIP

NBIP richt zich op de ontwikkeling van een open security platform dat geïntegreerd is in het modulaire edge datacenter. De bedoeling is de volgende generatie Europese datacenters secure by design te ontwerpen, zodat digitale weerbaarheid georganiseerd wordt daar waar het hoort, namelijk waar de applicaties, computing power en data zich bevinden.

In het afgelopen jaar hebben we de eerste stappen gemaakt omtrent het opzetten van een testbed. Dit testbed dient als een gecontroleerde omgeving waar nieuwe ideeën en technologieën op het gebied van cyberbeveiliging getest en geoptimaliseerd kunnen worden voordat ze worden uitgerold. Het biedt deelnemers de mogelijkheid om hun innovatieve concepten in de praktijk te brengen en te evalueren hoe effectief ze zijn in het tegengaan van cyberdreigingen.

Daarnaast heeft NBIP een aanzet gemaakt voor de ontwikkeling van gedecentraliseerde mitigatietechnieken. Dit houdt in dat in plaats van te vertrouwen op een gecentraliseerde infrastructuur, er een netwerk van gedistribueerde systemen wordt opgezet die gezamenlijk kunnen reageren op cyberaanvallen.

Op de zeepkist

In 2024 heeft NBIP op verschillende manieren haar kennis gedeeld binnen en buiten de sector. Zo gaven we diverse presentaties in binnen- en buitenland over onze diensten en projecten. Daarnaast hebben we bij verschillende media de missie van NBIP over het voetlicht kunnen brengen.

Artikelen, Interviews & Podcasts

Threat Talks — *DDoS Attacks on European Elections* ↗

Data Center Dynamics (DCD) — *The Edge in Action* ↗

ComputerWeekly — *Dutch working to promote cooperation in Europe to keep internet safe* ↗

Angry Nerds — *Tappen as a Service* ↗

All the Cyber Ladies ↗

AG Connect — *Zorgen over cyberaanvallen en kwetsbare computernetwerken zijn terecht, maar focus liever op oplossingen* ↗

AG Connect - *Nederlandse vinding voor extra DDoS-bescherming bijna live* ↗

Presentaties

DKNOG14 in Kopenhagen ↗

European Peering Forum ↗

Beyond 125 Years 'Securing our World's Digital Future and beyond' ↗

Women4Cyber Conference 'Beyond Borders' – *Het veranderende DDoS-landschap in geopolitieke context* ↗

Green Data Center Conference – *Modular Integrated Sustainable Datacenter* ↗

Terugblik derde editie

NBIP NEXT

Voor de derde keer organiseerde NBIP in 2024 haar jaarlijkse kennisevent NBIP NEXT. Het event is een uitgelezen mogelijkheid om praktische kennis te delen over alle activiteiten die aanbieders van digitale infrastructuur helpen om hun digitale weerbaarheid en naleving van wet- en regelgeving op orde te hebben.

Ruim 150 bezoekers meldden zich voor het event bij Kasteel De Hooge Vuursche in Baarn. Traditiegetrouw vond in de ochtend de deelnemersvergadering plaats, waarin de Raad van Deelnemers van NBIP bijeenkwam. Het middagprogramma was verdeeld in twee tracks: wet- en regelgeving in de praktijk (Track 1) en DDoS-mitigation (Track 2, Engelstalig).

De middag werd plenair geopend door Octavia de Weerdt, algemeen directeur van NBIP. Tijdens deze opening stond zij uitgebreid stil bij het 10-jarig jubileum van de NaWas, waarbij enkele betrokkenen van het eerste uur in het zonnetje werden gezet.

Het middagprogramma bestond uit een rijke variëteit aan sprekers, waaronder Jair Santanna (voormalig principal researcher Northwave Cybersecurity) en Arda Gerkens (bestuursvoorzitter ATKM). Bibi van Alphen (juridisch & public affairs adviseur Freedom Internet) beet het spits af met een gedetailleerd verhaal over de rechtszaak die onder meer Freedom in Europa voerde vanwege internetblokkades die ISP's sinds 2022 moeten handhaven.

Cyberbeveiligingswet (NIS2)

Ook werd tijdens NBIP NEXT uitgebreid ingegaan op de verplichtingen die Cyberbeveiligingswet (NIS2) met zich meebrengt, waaronder de meldplicht voor incidenten, de registratieplicht voor NIS2-entiteiten en de zorgplicht. Matthijs van Amelsfort (directeur Nationaal Cyber Security Centre, NCSC) en Esther Paalman van het ministerie van Economische Zaken gingen in op enkele verplichtingen maar ook de manier van samenwerking tussen overheid en de sector onder de nieuwe wetgeving.

Er was ook uitgebreid aandacht voor de laatste ontwikkelingen op het gebied van DDoS en DDoS-mitigatie. Zo werd teruggeblikt op 10 jaar DDoS-aanvallen en werd er een inkijk gegeven in een aantal casussen die zich in 2024 voordeden binnen NaWas. Daarnaast was er ook een update vanuit het academisch onderzoek naar DDoS en de internationale aanpak van booters waar de Nationale Politie aan bijdraagt.

Sectorsamenwerking cruciaal voor cyberweerbaarheid

Na het middagprogramma werden bezoekers nog kort toegesproken door Matthijs van Amelsfort. Het NCSC heeft een aantal belangrijke taken bij het uitvoeren van de cyberbeveiligingswet, waaronder incident response en het delen van dreigingsinformatie.

Aangezien met ingang van de wet 10.000 entiteiten onder het NCSC zullen vallen, waaronder een belangrijk gedeelte van de aanbieders van digitale infrastructuur in Nederland, was de boodschap van dat samenwerking tussen de sector, onder meer via NBIP, en het NCSC cruciaal is om Nederland cyberweerbaar te maken en te houden.

Meld je aan voor NBIP NEXT 2025

Op woensdag 26 november en donderdag 27 november organiseert NBIP voor de vierde keer NBIP NEXT. Vanwege de groeiende behoefte aan kennisdeling over Europese cyberweerbaarheid, DDoS-mitigatie en abuse bestrijding organiseren we nu een tweedaags event. De eerste dag zal in het teken staan van wet- en regelgeving en DDoS-mitigatie in samenwerking met de anti-DDoS-coalitie. De tweede dag is gericht op Europese samenwerking en strategische autonomie. Ook dit jaar vindt NBIP NEXT plaats op Kasteel De Hooge Vuursche.

Wil je het event niet missen?

Klik dan hier om jezelf aan te melden ↗

Over NBIP

De stichting Nationale Beheersorganisatie Internet Providers (NBIP) is in 2001 opgericht als uitvoeringsinstituut voor tapbevelen die voortvloeien uit de Telecommunicatiewet. Tegenwoordig is de NBIP uitgegroeid tot het expertisecentrum voor DDoS-mitigatie, Lawful Interception en Threat Intelligence-analyse voor internet-, hosting- en cloudproviders in Nederland en Europa.

NBIP heeft de missie om aanbieders van digitale infrastructuur te helpen aan hun operationele compliance te voldoen met diensten die efficiënt te exploiteren zijn. Deelnemers kunnen dure of complexe faciliteiten die ze niet de hele tijd nodig hebben gezamenlijk via NBIP gebruiken. Het bekendste voorbeeld hiervan is de Nationale Wasstraat (NaWas), het grootste non-profit DDoS scrubbing center ter wereld waarvan meer dan 130 organisaties in 9 Europese landen gebruikmaken. NBIP is door de jaren heen uitgegroeid tot een vaste waarde in het Nederlandse internetlandschap.

Met zo'n 200 deelnemers, een internationale aanwezigheid en betrokkenheid bij strategische Europese ontwikkelingstrajecten, is bewezen dat de filosofie van NBIP ook in de praktijk werkt. Zowel aanbieders van digitale infrastructuur als publieke en private partners weten hun weg naar NBIP te vinden.

Kijk voor meer informatie en actuele ontwikkelingen op nbip.nl

NBIP nationale beheersorganisatie internet providers